KENTUCKY LOTTERY CORPORATION
LOUISVILLE, KENTUCKY

MEMORANDUM OF COMMENTS
AND SUGGESTIONS

June 30, 2005

MOORE STEPHENS POTTER LLP

CERTIFIED PUBLIC ACCOUNTANTS • BUSINESS ADVISORS

August 19, 2005

To Management of the
Kentucky Lottery Corporation
Louisville, Kentucky

In planning and performing our audit of the financial statements of the Kentucky Lottery Corporation (KLC) for the year ended June 30, 2005, we considered the KLC's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control.

However, during out audit we became aware of matters which are opportunities for strengthening internal controls and operating efficiency. This letter does not affect our report dated August 19, 2005 on the financial statements of the Kentucky Lottery Corporation. Summarized below are our suggestions that we believe warrant your attention.

* * * * * *

VIRUS PROTECTION

With the increased use of the network as a key component of KLC's operations, it is necessary that KLC be vigilant in its protection against malicious or destructive code, such as viruses, worms, Trojan horses, logic bombs, and other "uninvited" software also referred to as malware. Malware has become the most significant external threat against most systems, causing widespread damage and disruption, and extensive recovery efforts within most organizations. KLC uses an enterprise based anti-virus system to protect against these types of threats. However, not all of the systems are updated automatically when new threats are identified. Automatic updates are obtained from the virus protection site hourly and many of the servers are only updated when time permits to manually update them.

KLC should use centrally managed antivirus software that is controlled and monitored regularly by system administrators, who are also responsible for acquiring, testing, approving, and delivering antivirus signature and software updates throughout the organization. Antivirus administrators should perform periodic checks to confirm that systems are using current antivirus software and that the software is configured properly. This information is available through KLC's antivirus management software. Implementing all of these recommendations should strongly support an organization in having a strong and consistent antivirus deployment across the organization.

Management's response:

Management agrees with the comment and is in process of centralizing all antivirus updates. Since this effort will require Network Services to visit each region for manual installation, this process is contingent upon the refresh and replacement of KLC desktop units, and upon priority SWAT activities. Completion is expected by the end of the fiscal year, June 30, 2006.

SERVER AND APPLICATION CONFIGURATION MANAGEMENT

Server and application updates and configurations play a key role in securing information systems. The servers provide a number of services that are used by the organization including financial information. Despite extensive testing, all operating systems and applications are released with errors in the software that affect security, performance, and stability of the system. The software manufacturer often releases a piece of software to correct the errors. This software is often called a patch, hotfix, or service pack.

Patches are usually released for four reasons:

- To fix faults in an application or operating system.
- Patches are also released to correct performance or functionality problems.
- To alter functionality or to address a new security threat.
- To change or modify the software configuration to make it less susceptible to attacks and more secure.

Timely patching is critical to maintaining the operational availability, confidentiality, and integrity of the information technology systems, both on the network and the AS400.

Vulnerabilities are weaknesses in software that can be exploited by a malicious entity to gain greater access and/or permission than it is authorized to have on a computer. Not all vulnerabilities have related patches; thus, system administrators must not only be aware of vulnerabilities and patches, but also mitigate “unpatched” vulnerabilities through other methods (e.g. workarounds, firewalls, and router access control lists). An attacker only needs one point of access to compromise a network.

To help address this growing problem, we recommend that the organizations have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.

Management's response:

IT management agrees with the recommendation and has made remediation of this issue the KLC’s highest IT priority. On July 29, 2005, a cross-functional group was assigned to develop a project plan and timetable for resolution which would provide the most immediate improvement to the KLC’s computing infrastructure. The plan and timeline establishes the following:

- All appropriate and applicable security patches will be installed by November 30, 2005. This initial focus on the patches will eliminate known vulnerabilities, ensuring the accuracy and integrity of the systems and data.
- Software for which newer versions are available will be upgraded as appropriate and applicable by September 30, 2006. The upgrades and the order in which they will be addressed are being determined using a risk-based approach, which will ensure that critical and/or security-sensitive areas are addressed first.
- A patch management and change control policy will be developed and documented by the November 30, 2005, patching deadline in order to ensure that patches are applied regularly and timely in the future.
- The Network Services Manager and Director of Operations have been given the responsibilities of project leader and project manager, respectively, and now report directly to the organization’s Chief Operating Officer.

SOFTWARE ESCROW

Current versions of the software provided by GTECH are stored in the escrow facility. Currently, the software that is stored in the escrow facility is not tested. We recommend that all software stored in escrow be periodically tested to assure that the copies are usable.

Management's response:

KLC's Information Security personnel are rewriting the software escrow policy and will determine what software to escrow based on a risk assessment. We will address the testing issue as part of this process, with the new policy, including any provision for testing the escrowed software, will be implemented by October 31, 2005.

GTECH

GTECH has an internal server with a Windows NT 4.0 operating system. Microsoft no longer supports this operating system. The server is used internally to run CISCO Works, a network monitoring tool. Because Microsoft is no longer supporting this operating system, security updates will not be provided. GTECH should migrate this machine to a supported operating system.

Management's response:

There is not an issue with upgrading or replacing the workstation in question to support a later version of Microsoft's operating systems. It has not yet been determined if our current version of CISCO Works will function on Windows 2000 or 2003. Once we determine the limitations of our CISCO Works software a date will be set for the upgrade. If this software is incompatible with the later versions of Windows we can either upgrade or find a suitable replacement.

BACKUP SITE TELECOMMUNICATION CABLING

Telecommunication Cabling at the Commonwealth Office of Technology (COT) in Frankfort, KY is secured within the data center and inside the cage containing KLC's equipment by metal conduit. However, after exiting the cage and when entering the telecommunications room within the data center, the cabling is exposed between entering the room and entering the panel box. The panel box itself is secured by a tamper evident band. This leaves the cabling exposed to tampering within telecommunications room. There are no camera's installed within this telecommunications room to detect unauthorized activity. The telecommunications room is normally locked, however, during our visit, the door to this room was propped open and unattended for at least thirty minutes during our review of the site. Both MS Potter and KLC were able to access the room without monitoring from anyone at COT.

According the current draft of KLC's Information Security Policy, dated June 30, 2005, Section 7.2.3 indicates that telecommunications will be protected from interception or damage by conduit or by avoiding public areas. Although this would not be considered a public area, the lack of monitoring of activity within the telecommunications room would predicate that the cabling should be secured within conduit in this area. We recommend the cabling be installed within protective cabling.

Management's response:

Management agrees with the comment and recommendation, and, in conjunction with the Commonwealth of Kentucky Office of Technology data center management, is taking steps to control access to the telecommunications wiring closet, and to enclose the KLC data communications cables within steel conduit, in accordance with security policies of both entities. Completion of the KLC portion of these issues for compliance with the KLC Information Security Policy is expected by February 28, 2006.

USER ACCESS LEVELS

User system access levels for the AS 400 system are reviewed on a quarterly basis by the Information Security Officer. However, there are no written procedures explaining the system level access to be granted for various users and their roles or departments. Currently, the review is a comparison of previously granted access to the current access. To improve user access control, we recommend user rights levels be documented in writing according to job function, restricting unnecessary or excessive access whenever possible. As KLC continues to expand its technologies and incorporates more open system technologies, the control of the legacy AS400 systems needs to be reassessed to improve the security infrastructure.

Management's response:

The KLC's IS personnel will document the system access which has been granted to users based on users' job responsibilities and needs as indicated by the applicable department head. All future system access will be granted using these models. Any deviations or special authorities will be documented and approved by the department head, the ISO, and the data owner, as applicable. This will be in place by December 31, 2005.

* * * * * *

STATUS OF PRIOR YEAR COMMENTS AND SUGGESTIONS

The status of the comments made during the audit for the year ended June 30, 2004 are as follows:

BUSINESS CONTINGENCY AND SERVICE CONTINUITY

PLAN UPDATES

The Business Continuity Plan Maintenance Policy indicates that updates will be according to the schedule in the policy. For example, information regarding essential employees in the plan will be updated immediately. The Business Continuity Plan Administrator terminated employment in May 2004 and her information is still in the plan. Secondly, the new Accounts Receivable system is not documented for recovery within the plan document. We recommend these updates be completed as soon as possible.

2005 update:

- Plans were updated including AR.
- Department approval in process.
- Executive approval not complete.

BUSINESS CONTINGENCY TEST

A disaster recovery test was scheduled for May 2004 using a toxic biohazard scenario. However the test had to be postponed. Testing rescheduled for September or October 2004. We recommend this test be performed and documented to facilitate a thorough recovery process.

2005 update:

- Test was performed successfully.

NETWORK AUDIT

ACCOUNTS RECEIVABLE INTERFACE

The Accounts Receivable system interfaces the Accounts Receivable database on the AS400. This connectivity through the Intel network increases the need for information security auditing of the Intel network. The Information Security department is manually reviewing activity on these systems, however, the new Accounts Receivable system has greatly increased the operational burden of these reviews. Currently, the Information Security Officer also uses a Novell Netware tool, AuditCon, to assist in this process. The AuditCon program does not provide for independent auditing functions in that the network administrators have the ability to circumvent the audit system and prevent the Information Security Officer from identifying inappropriate use of the system. Information Security has already designated a different audit tool, BindView, to assist in the information security audit function. We recommend Information Security implement this process as soon as possible.

2005 update:

- Network is significantly behind on its software versions. See comment re server and application configuration management above.

SPECIAL AUTHORITIES

During our audit procedures for special authority access for the AS 400 system, we noted requests for special authority access are not provided in writing. We also noted special authority access is controlled via password maintained by the Information Security Officer. However, the password changes monthly so users who have obtained the password will have access to the special authority profile for the remainder of the month.

In order to provide audit trail documentation for special authority access, we suggest all requests be provided in writing. This is also mentioned in KLC IT Policy 2 - Requests to Operations. We also suggest the password for the special authority profile be changed weekly to limit the possibility for potential misuse.

2005 update:

- Requests for special authority access are now required to be provided in writing.
- The special authority access profile password is now changed every two weeks and upon use by anyone outside of information security.

USER RIGHTS ADMINISTRATION

As security becomes more complicated, it is important that the security over the AS400’s be controlled and monitored. Findings in this audit regarding excessive object access, maintenance of security profiles, and audit of security issues on the AS400’s continues to indicate the need for the improved security. Also, the increased use of the Intel network demands enhanced security of user access on this network. The Lottery should continue to assess the user rights for all users on a role based approach, granting only the access necessary for the employee to perform the job function for each of the systems.

2005 update:

- Bindview is now implemented.

* * * * * *

We will review the status of the above comments during our next audit engagement. We will also be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

This report is intended solely for the information and use of the KLC's management and is not intended to be and should not be used by anyone other than these specified parties.

Moore Stephens Potter, LLP

MOORE STEPHENS POTTER, LLP